INCIDENT REPORT 2023

Premium House Lights

Email: admin@premiumhouselights.com

Website: premiumhouselights.com

Report by Jasraj Johal (Junior Security Analyst)

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Financial Highlights

The headings are typical annual report headings that you might want to use as-is.

Operating Highlights

Think a document that looks this good has to be difficult to format? Think again! To easily apply any text formatting you see in this document with just a tap, on the Home tab of the ribbon, check out Styles.

"Got something very important to point out to your readers? Use this bar to make it stand out."

Looking Ahead

View and edit this document in Word on your computer, tablet, or phone. You can edit text; easily insert content such as pictures, shapes, and tables; and seamlessly save the document to the cloud from Word on your Windows, Mac, Android, or iOS device.

Chief Executive Name
Chief Executive Title
Date

FINANCIAL SUMMARY

Use this section to give a brief summary of your financials, highlighting important points. Some of the sample text in this document indicates the name of the style applied, so that you can easily apply the same formatting again.

- For example, this is the List Bullet style.
- Here is another sentence formatted in List Bullet style.

You can find easy-to-use tools on the Insert tab, such as to add a hyperlink, insert a comment, or add automatic page numbering.

View and edit this document in Word on your computer, tablet, or phone. You can edit text; easily insert content such as pictures, shapes, and tables; and seamlessly save the document to the cloud from Word on your Windows, Mac, Android, or iOS device.

FINANCIAL STATEMENTS

Statement of Financial Position

- Liabilities
- Statement of Financial Position
- Ownership Equity

Statement of Comprehensive Income (Profits and Losses)

- Income
- Expenses
- Profits

Statement of Changes in Equity

Well, it wouldn't be an annual report without a lot of numbers, right? This section is the place for all those financial tables.

To get started with a table that looks just like the sample here, on the Insert tab, tap Table.

DESCRIPTION	REVENUE	EXPENSES	EARNINGS

Statement of Cash Flows

- Operating
- Investing
- Financing

NOTES TO FINANCIAL STATEMENTS

Accounts

When you have a document that shows a lot of numbers, it's a good idea to have a little text that explains the numbers. You can do that here.

Debt

Of course, we would all prefer to just have profits. But if you've got any debt, this is the place to make notes about it.

Debt

Of course, we would all prefer to just have profits. But if you've got any debt, this is the place to make notes about it.

Going Concern

Okay, you get the idea. If you've got notes to add about your financials, add them here.

"Strong Caption Goes Here. Write Something in This Caption Holder."

Contingent Liabilities

Keep in mind that some of these headings might not apply to your business (and you might have others to add). This one, for example, is about potential liabilities that could arise if something happens in the future, such as a pending legal decision.

Takeaways

What would you like your readers to understand? Add notes on key takeaways here.

INDEPENDENT AUDITOR'S REPORT

Auditor's Report

- Unqualified Opinion
- Qualified Opinion Report
- Adverse Opinion Report
- Disclaimer of Opinion Report
- Auditor's Report on Internal Controls of Public Companies
- Going Concern

Reconnaissance started at Sun, 20 Feb 2022 02:58:22 GMT.

Wireshark · Follow TCP Stream (tcp.stream eq 134) · phl_webserver.pcap

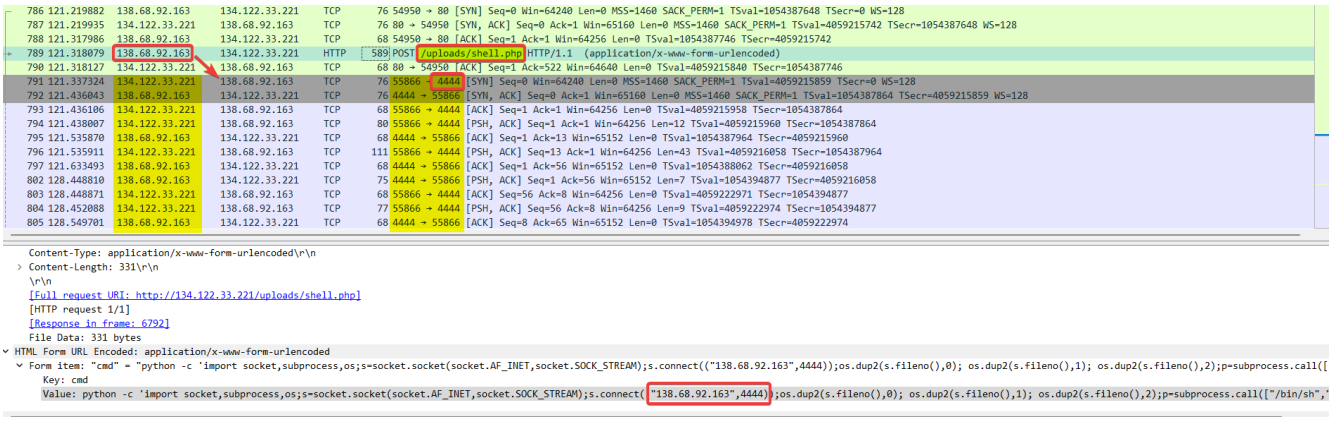
```
GET /randomfile1 HTTP/1.1
Host: 134.122.33.221
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Accept: */*

HTTP/1.1 404 Not Found
Date: Sun, 20 Feb 2022 02:58:22 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 276
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at 134.122.33.221 Port 80</address>
</body></html>
```

Attacker uploading shell.php.

Source	Destination	Protocol	Length	Info
134.122.33.221	138.68.92.163	HTTP	505	HTTP/1.1 404 Not Found (text/html)
138.68.92.163	134.122.33.221	HTTP	199	GET /uploads/frand2 HTTP/1.1
134.122.33.221	138.68.92.163	HTTP	505	HTTP/1.1 404 Not Found (text/html)
138.68.92.163	134.122.33.221	HTTP	193	GET /uploads/ HTTP/1.1
134.122.33.221	138.68.92.163	HTTP	1183	HTTP/1.1 200 OK (text/html)
138.68.92.163	134.122.33.221	TCP	68	54946 → 80 [FIN, ACK] Seq=10879 Ack=39277 Win=64128 Len=0 TSval=1054364486 TSecr=4059192481
134.122.33.221	138.68.92.163	TCP	68	80 → 54946 [FIN, ACK] Seq=39277 Ack=10880 Win=64256 Len=0 TSval=4059192580 TSecr=1054364486
138.68.92.163	134.122.33.221	TCP	68	54946 → 80 [ACK] Seq=10880 Ack=39278 Win=64128 Len=0 TSval=1054364584 TSecr=4059192580
138.68.92.163	134.122.33.221	TCP	76	54948 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1054379185 TSecr=0 WS=128
134.122.33.221	138.68.92.163	TCP	76	80 → 54948 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=4059207281 TSecr=1054379185 WS=128
138.68.92.163	134.122.33.221	TCP	68	54948 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1054379285 TSecr=4059207281
138.68.92.163	134.122.33.221	HTTP	154	GET /uploads/ HTTP/1.1
134.122.33.221	138.68.92.163	TCP	68	80 → 54948 [ACK] Seq=1 Ack=87 Win=65152 Len=0 TSval=4059207380 TSecr=1054379286
134.122.33.221	138.68.92.163	HTTP	1183	HTTP/1.1 200 OK (text/html)
138.68.92.163	134.122.33.221	TCP	68	54948 → 80 [ACK] Seq=87 Ack=1116 Win=64128 Len=0 TSval=1054379384 TSecr=4059207380
138.68.92.163	134.122.33.221	TCP	68	54948 → 80 [FIN, ACK] Seq=87 Ack=1116 Win=64128 Len=0 TSval=1054379385 TSecr=4059207380
134.122.33.221	138.68.92.163	TCP	68	80 → 54948 [FIN, ACK] Seq=1116 Ack=88 Win=65152 Len=0 TSval=4059207478 TSecr=1054379385
138.68.92.163	134.122.33.221	TCP	68	54948 → 80 [ACK] Seq=88 Ack=1117 Win=64128 Len=0 TSval=1054379482 TSecr=4059207478
138.68.92.163	134.122.33.221	TCP	76	54950 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1054387648 TSecr=0 WS=128
134.122.33.221	138.68.92.163	TCP	76	80 → 54950 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=4059215742 TSecr=1054387648 WS=128
138.68.92.163	134.122.33.221	TCP	68	54950 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1054387746 TSecr=4059215742
138.68.92.163	134.122.33.221	HTTP	589	POST /uploads/shell.php HTTP/1.1 (application/x-www-form-urlencoded)
134.122.33.221	138.68.92.163	TCP	68	80 → 54950 [ACK] Seq=1 Ack=522 Win=64640 Len=0 TSval=4059215840 TSecr=1054387746
134.122.33.221	138.68.92.163	TCP	76	55866 → 4444 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4059215859 TSecr=0 WS=128



The script used to shell

Is attached/hyperlinked: shell_contents